REMARKS

Applicant respectfully requests entry of the foregoing amendments and reconsideration of the merits of the outstanding rejections in view of the following remarks. Claims 1-54 are currently pending.

I. Interview

At the outset, the undersigned thanks the Examiner for the courtesies extended during the telephone interview conducted on October 13, 2005.

II. Allowable Subject Matter

Applicant notes with appreciation the indication on page 10 of the Office Action that claims 5, 6, 13, 14, 17-19, 23, and 24 are allowed, and that claims 7-10, 34, 35, 44, and 45 are allowable if rewritten in independent form. Applicant has rewritten claims 7, 44, and 45 in independent form; claims 8-10 depend from claim 7.

Applicant has opted to defer rewriting claims 34 and 35 in independent form pending reconsideration of the arguments presented below with respect to the rejected independent claims.

III. The Obviousness Rejection

Claims 1-4, 11, 12, 15, 16, 20-22, 25-33, 36-43, and 46-54 stand rejected under 35 U.S.C. § 103(a), as allegedly unpatentable over "AppShield Provides Block Against Application Hacks," Report on Electronic Commerce, BRP Publications (referred to as "BRP Publications" within the Office Action) in view of U.S. Patent No. 6,584,569 to Reshef *et al.* ("Reshef"). Office Action at page 2. Particularly, the Examiner contends that BRP publications teaches all of the claim limitations except for "designating an application path of an application as restricted." *Id.* In an attempt to cure this deficiency, Reshef is introduced as allegedly disclosing this element. *Id.* The Examiner then opines that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to include the application path of the application as restricted with BRP publications, the motivation is that the detection phase searches for application path parameters in order to check for a vulnerability (see col. 3, lines 60-67)." *Id.* Applicant respectfully disagrees and traverses this rejection at least on the following grounds.

a. Proposed Combination Would Render AppShield Unsatisfactory For Its Intended Purpose or Would Change Its Principle of Operation

Applicant respectfully submits that the proposed combination is not sufficient to render the claims prima facie obvious because the combination would render BRP Publications, i.e., AppShield, unsatisfactory for its intended purpose or would change its principle of operation.

As stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Further, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

i. AppShield Utilizes a Dynamic Security Policy to Prevent Hacking Attempts

The BRP Publication vaguely describes an Internet application for security, referred to as "AppShield." *See* BRP Publication, lines 13-14. AppShield implements a dynamic security policy that is generated from examination of the HTML body of every outgoing web page. *See id.* at lines 23-25 ("AppShield recognizes the intended application security policy by analyzing each outbound hypertext markup language (HTML) page"). Any subsequent incoming request is then checked against that dynamic policy. *See id.* at lines 25-26 ("Then it enforces compliance with the policy for each incoming hypertext transfer protocol (HTTP) application"). If a subsequent incoming request is unexpected in view of the dynamic security policy, that request is rejected. *See id.* at lines 30-32 ("AppShield rejects unexpected - and therefore illegal - inputs, generating an error page for the user and notifying the AppShield management log."). AppShield therefore attempts to prevent attacks as they occur through enforcement of the dynamic policy. *See id.* at lines 27-29 ("AppShield protects the integrity of an e-commerce application by making it nearly impossible for hackers to use traditional security loopholes, either in the applications code or within Web servers.").

ii. Reshef is Directed to Scanning for Application Vulnerabilities

Reshef is directed toward a system for determining web application vulnerabilities. *See* Reshef, abstract. Particularly, Reshef scans for vulnerabilities by attacking a web application in

a simulation mode. *See id.* at col. 2, lines 24-28 ("Then, based on a pre-defined set of hacking rules or techniques, the scanner mutates client requests in various ways, thereby generating exploits that will be unique for each web application. These exploits may then be used to attack the web application.") Reshef then reports the results of the attack to a user so that possible vulnerabilities may be fixed before a real attack occurs. *See id.* at col. 4, lines 27-29 ("The scanner 10 preferably also provides a report 402 recommending fixes or other pertinent advice concerning each detected vulnerability.").

Reshef's scanner only identifies vulnerabilities, it does not, by itself, prevent those vulnerabilities from being exploited by hackers.

iii. AppShield and Reshef are Inoperable Together

AppShield and Reshef are inoperable together. As discussed above, AppShield operates utilizing a dynamic security policy and attempts to prevent attacks while they occur. Because AppShield's dynamic policy is generated "on-the-fly" from outgoing web pages, it does not utilize any information pertaining to vulnerabilities pre-identified through a scanning mechanism. In contrast, Reshef utilizes a scanning mechanism to merely identify possible vulnerabilities, which are presented in a "static" report to the user.

Because AppShield and Reshef are inoperable together, adding a scanning phase from Reshef into AppShield, would either render AppShield unsatisfactory for its intended purpose or would change its principle of operation. As noted, AppShield does not employ a security policy based on the results of a vulnerability scan, but rather generates its own dynamic policy "on-the-fly."

Accordingly, Applicant respectfully submits that the obviousness rejection is improper and requests the Examiner to withdraw the rejection of claims 1-4, 11, 12, 15, 16, 20-22, 25-33, 36-43, and 46-54.

b. The Proposed Combination Does Not Teach or Suggest All of the Claim Limitations

Applicant also respectfully submits that the proposed combination does not teach or suggest all of the limitations recited in the claims.

As stated in MPEP § 2143.01, to establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the

patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

i. Claims 1-4, 11, 12, 15, 16, 20-22, 25, and 26

Although Applicant maintains that the basis of the obviousness rejection is unsound in view of the claims as previously presented, the independent claims have been amended to better describe the claimed invention. Particularly, claim 1 as currently amended recites:

> 1. A method for protecting an application from executing an illegal or harmful operation request received from a distrusted or trusted environment, the method comprising the steps of:
>
> designating an application path of an application as restricted,
>
> *matching an operation request to said application path, wherein said application path is a virtual directory or a subdirectory of said application*,
>
> determining whether said operation request is illegal or harmful to an environment of said application *according to security settings designated for said application path*, and
>
> preventing said application from executing said operation request. (Emphasis added.)

Support for this amendment is found at least at page 10, lines 7-10; page 13, line 29 to page 14, line 13; and Fig. 3 of the Applicant's Specification.

Applicant respectfully submits that BRP Publications, either taken alone or in combination with Reshef, fails to teach or suggest the steps of "matching an operation request to said application path, wherein said application path is a virtual directory or a subdirectory of said application" and "determining whether said operation request is illegal or harmful to an environment of said application according to security settings designated for said application path" as recited in currently amended independent claim 1. BRP Publications, i.e., AppShield, checks subsequent incoming requests against a dynamic policy derived from outgoing web pages. *See* BRP Publications at lines 21-26. AppShield does not match an operation request to any application path whatsoever, namely one that it is a virtual directory or a subdirectory of said application. Moreover, AppShield does not designate security settings for an application path and scrutinizing an operation request according to those designated security settings. As noted above, Reshef is directed to a vulnerability scanner and has nothing to do with protecting (i.e.,

preventing) an application from executing an illegal or harmful request. Accordingly, Reshef fails to cure the deficiencies presented by AppShield.

Because all the claim limitations are not taught or suggested by the prior art, amended independent claim 1 is nonobvious, and all claims dependent therefrom, *e.g.*, claims 2-4, 11, 12, 15, 16, 20-22, 25, and 26, are also nonobvious.

Although dependent claims 2-4, 11, 12, 15, 16, 20-22, 25, and 26 are allowable at least by virtue of their dependency on independent claim 1, these claims recite additional subject matter which is not suggested by the cited art taken either alone or in combination. For instance, claim 11 recites (and claim 15 similarly recites) "comparing said operation request against stored known vulnerability patterns to determine a match; and blocking said operation request if said match is found." Reshef does not teaching or suggest "blocking ..." as the Examiner otherwise contends. *See* Office Action at page 3. As noted above, Reshef merely identifies possible vulnerabilities through its scanning mechanism and does nothing, on its own, to fix the vulnerability. *See, e.g.*, Reshef at col. 4, lines 27-29 ("The scanner 10 preferably also provides a report 402 recommending fixes or other pertinent advice concerning each detected vulnerability."). Reshef's vulnerability scanner has nothing to do with protecting an application from an attack as it occurs, for example, by blocking an operation request. Likewise, Reshef does not teach or suggest "updating said stored vulnerability patterns with newly found vulnerability patterns" as recited in claim 12. Reshef may give a report of identified possible vulnerabilities, but Reshef, itself, does not take any assertive action to address those vulnerabilities, for instance, by updating a list of vulnerability patterns that would be used in a prevention mechanism to proactively scrutinize operation requests as they are received from a distrusted source as claimed. Moreover, as the Examiner correctly notes, AppShield does not implement "stored vulnerability patterns." *See* Office Action at page 4. Because a dynamic security policy is employed, AppShield's principle of operation would have to be changed to implement "stored vulnerability patterns." *See* Remarks III(a)(iii), *supra*.

For at least the reasons set forth above, Applicant submits that the instant rejection of claims 1-4, 11, 12, 15, 16, 20-22, 25-33, 36-43, and 46-54 is unsustainable.

ii. Claims 27-33, 36-43, 46, and 47

Amended claim 27 recites "matching each operation request to an application path, wherein said application path is a virtual directory or a subdirectory of said application; and

determining whether each operation request is illegal or harmful to an environment of said application," which is a similar recitation as found in amended claim 1. Therefore, Applicant respectfully submits that claim 27 is nonobvious at least for the reasons remarked above with respect to claim 1. *See* Remarks III(a)(iii) and III(b)(i), *supra*.

Although dependent claims 28-33, 36-43, 46, and 47 are allowable at least by virtue of their dependency on independent claim 27, these claims recite additional subject matter which is not suggested by the cited art taken either alone or in combination. For instance, claim 32 recites (and claim 36 similarly recites) "comparing said operation request against stored known vulnerability patterns to determine a match; and blocking said operation request if said match is found" *See* Remarks III(b)(i), *supra*. Likewise, Reshef does not teach or suggest "updating said stored vulnerability patterns with newly found vulnerability patterns" as recited in claim 33. *Id.*

For at least the reasons set forth above, Applicant submits that the instant rejection of claims 27-33, 36-43, 46, and 47 is unsustainable.

iii. Claims 48-54

Independent claims 48 and 51 each recite a "means for embedding said operation request into a data format used by said application." BRP Publications does not teach or suggest this limitation as the Examiner otherwise contends on page 9 of the Office Action. BRP Publications does not even touch on the subject of embedding operation requests into another data format, particularly one used by an application. The Examiner's cited passage (i.e., lines 30-33) merely states that "AppShield rejects unexpected - and therefore illegal - inputs, generating an error page for the user and notifying the AppShield management log." BRP Publications fails to provide the specificity needed to render these claims obvious.

Likewise, claims 48 and 51 recite or similarly recite a "means for ascertaining an application path of said operation request" and a "means for checking a contents of said operation request according to a predefined set of rules associated with said ascertained application path to identify if said operation request is illegal or harmful to an environment of said application." BRP Publications, either taken alone or in combination with Reshef, fails to teach or suggest this limitation. Remarks III(b)(i), *supra*.

Dependent claims 49, 50, and 52-54 are allowable at least by virtue of their dependency on independent claim 48 or 51.

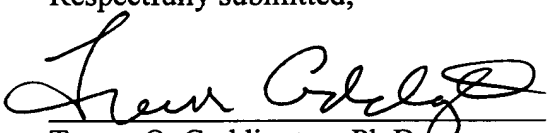
For at least the reasons set forth above, Applicant submits that the instant rejection of claims 48-54 is unsustainable.

IV. Conclusion

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

Applicant is concurrently filing herewith an RCE and a Petition for a Two-Month Extension of Time, along with the requisite fees. In the event that the U.S. Patent and Trademark Office requires additional fees to enter and/or consider this Reply, or to prevent abandonment of the present application, please charge such fees to the undersigned's Deposit Account No. 50-2613.

Respectfully submitted,

October 27, 2005 By: 

Trevor Q. Coddington, Ph.D.
Registration No. 46,633

PAUL, HASTINGS, JANOFSKY & WALKER LLP
Customer Number: 36183
P.O. Box 919092
San Diego, CA 92191-9092
Telephone: (858) 720-2500
Facsimile: (858) 720-2555

(202) 955-1500 (telephone)
(202) 778-2201 (facsimile)